Daily brief, Thursday, June 4, 2026

Jun 3, 8:00 PM to Jun 4, 8:00 PM ET

Generated Nov 5, 2026, 8:14 AM ET

0	0	0	75	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

75 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

75

10.0 **CVE-2026-48567** Microsoft azure horizondb

Authentication bypass by spoofing in Azure HorizonDB allows an unauthorized attacker to elevate privileges over a network.

9.6 **CVE-2026-10881** Google chrome

Out of bounds read and write in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-10886** Google chrome

+1 more CVEs in the same release

Use after free in FileSystem in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-10892** Google chrome

Out of bounds write in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.6 **CVE-2026-10966** Google chrome

Inappropriate implementation in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: High)

9.6 **CVE-2026-10971** Google chrome

Insufficient validation of untrusted input in Printing in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security sev

9.6 **CVE-2026-10972** Google chrome

Use after free in Ozone in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-10974** Google chrome

+1 more CVEs in the same release

Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-10983** Google chrome

Insufficient validation of untrusted input in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-10990** Google chrome

Use after free in Glic in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-11002** Google chrome

Use after free in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-11009** Google chrome

Use after free in USB in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-11021** Google chrome

Insufficient validation of untrusted input in GPU in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity

9.6 **CVE-2026-11029** Google chrome

Insufficient validation of untrusted input in Drag and Drop in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium securit

9.6 **CVE-2026-11037** Google chrome

Out of bounds write in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)

9.6 **CVE-2026-11043** Google chrome

Out of bounds write in ANGLE in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-11047** Google chrome

Inappropriate implementation in Base in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-11052** Google chrome

Type Confusion in GPU in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

9.6 **CVE-2026-11056** Google chrome

Insufficient validation of untrusted input in SiteIsolation in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium securit

9.6 **CVE-2026-11061** Google chrome

Type Confusion in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)

53 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches

No new breaches published.

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. CVE IDs link to the full record on Watch Floor.